

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-340965

(43) 公開日 平成11年(1999)12月10日

(51) Int.Cl.⁹
H 0 4 L 9/08
G 0 6 F 13/00 3 5 1
G 0 9 C 1/00 6 4 0
H 0 4 L 9/32

F I
H 0 4 L 9/00 6 0 1 Z
G 0 6 F 13/00 3 5 1 G
G 0 9 C 1/00 6 4 0 B
H 0 4 L 9/00 6 0 1 E
6 7 5 B

審査請求 未請求 請求項の数 8 O L (全 11 頁) 最終頁に続く

(21) 出願番号 特願平10-148119
(22) 出願日 平成10年(1998) 5月28日

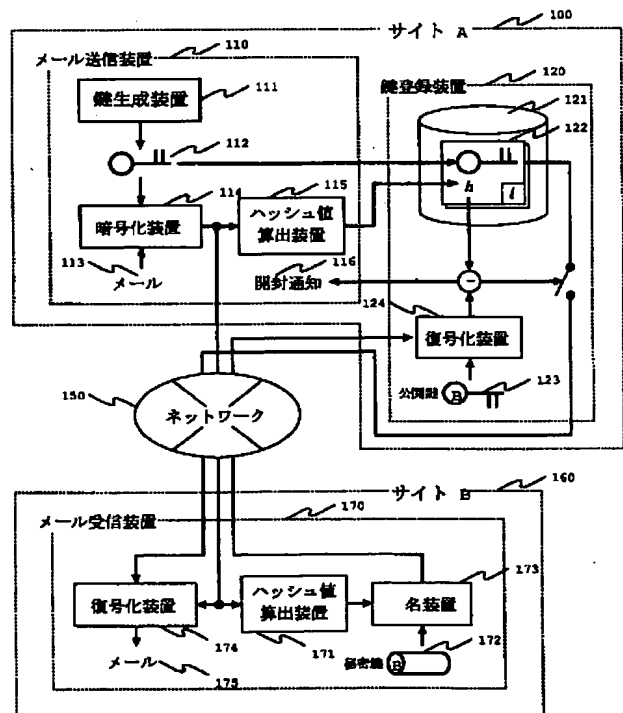
(71) 出願人 000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目 6 番地
(72) 発明者 仙石 浩明
神奈川県川崎市麻生区王禅寺1099番地 株
式会社日立製作所システム開発研究所内
(72) 発明者 市川 芳明
茨城県日立市大みか町五丁目 2 番 1 号 株
式会社日立製作所大みか工場内
(74) 代理人 弁理士 矢島 保夫

(54) 【発明の名称】 電子メール鍵登録装置、電子メール送信装置、電子メール受信装置、および電子メールシステム

(57) 【要約】

【課題】 インターネット等における電子メールシステムにおいても、閉じたネットワーク同様の機能、すなわち送信人が送信した電子メールが正しく受信人に届けられたか確認する機能、受信人がその内容を読んだか確認する機能、および電子メールの取り消し等の制御機能を提供することを目的とする。

【解決手段】 メール送信装置において、電子メールの送信操作を行なうたびに鍵を生成し、この鍵を用いて電子メールを暗号化し受信人に送信するとともに、その電子メールのメッセージ ID と鍵を鍵登録装置に鍵登録要求として送信する。鍵登録装置では、鍵登録要求にしたがって、各々の電子メール固有のメッセージ ID をキーとして鍵を登録する。電子メール受信装置では、受信人が閲覧操作を行なったとき、受信した電子メールに対応する鍵を前記鍵登録装置に対して自動的に要求する。その鍵取得要求に対して、鍵登録装置は、登録されている鍵を受信人に送る。電子メール受信装置は、取得した鍵を用いて電子メールを復号化する。



【特許請求の範囲】

【請求項 1】電子メールの送信人からの要求にしたがって、各々の電子メール固有のメッセージ ID をキーとして鍵を登録し、または削除する手段と、
鍵が削除されていない場合に限り、電子メールの受信人からの要求にしたがって、登録されている鍵を前記受信人に送る手段と、
登録された鍵それぞれについて、前記受信人が鍵を要求したか否かを前記送信人に通知する手段とを備えたことを特徴とする電子メール鍵登録装置。

【請求項 2】電子メールの送信人が電子メールの送信操作を行なうたびに鍵を生成し、この鍵を用いて電子メールを暗号化し受信人に送信する手段と、
前記電子メールのメッセージ ID と前記鍵を請求項 1 に記載の鍵登録装置に鍵登録要求として送信する手段と、
前記鍵登録装置からの通知に基づいて、送信済みの電子メールそれぞれについて、受信人が鍵を要求したか否かを表示する手段と、
受信人が鍵を未だ要求していない電子メールについては、送信人が取消操作を行なうと、この鍵の削除要求を鍵登録装置へ送り、受信人が読むことを不可能にする手段とを備えたことを特徴とする電子メール送信装置。

【請求項 3】請求項 2 に記載の送信装置によって暗号化され送信された電子メールを受信する電子メール受信装置であって、
受信人が閲覧操作を行なったとき、受信した電子メールに対応する鍵を前記鍵登録装置に対して自動的に要求し、該鍵を取得する手段と、
取得した鍵を用いて電子メールを復号化する手段とを備えたことを特徴とする電子メール受信装置。

【請求項 4】前記暗号化した電子メールのハッシュ値を算出し、このハッシュ値を、メッセージ ID および鍵と共に鍵登録要求として前記鍵登録装置に送信することを特徴とする、請求項 2 に記載の電子メール送信装置。

【請求項 5】受信人が閲覧操作を行なったとき、受信した電子メールのハッシュ値を受信人固有の秘密鍵を使って暗号化したものを、前記電子メールのメッセージ ID と共に鍵要求として、前記電子メールに対応する鍵登録装置に送信することを特徴とする、請求項 3 に記載の電子メール受信装置。

【請求項 6】請求項 4 に記載の電子メール送信装置が送信したメッセージ ID、鍵、およびハッシュ値を受信し、前記メッセージ ID をキーとして前記鍵およびハッシュ値を記録し、
請求項 5 に記載の電子メール受信装置が送信したメッセージ ID、および暗号化されたハッシュ値を受信し、前記暗号化されたハッシュ値を受信人の公開鍵を用いて復号化したものが、前記メッセージ ID をキーとして検索を行なって取り出したハッシュ値と一致するときに限り、検索を行なって取り出した鍵を前記電子メール受信

装置に送信し、

前記電子メール送信装置が送信したハッシュ値と、前記電子メール受信装置が送信した暗号化されたハッシュ値を復号化したものが一致したか否かを前記電子メール送信装置に伝えることを特徴とする、請求項 1 に記載の電子メール鍵登録装置。

【請求項 7】請求項 1、2、3 または請求項 4、5、6 に記載の、電子メール鍵登録装置、電子メール送信装置、および電子メール受信装置を含むことを特徴とする、電子メールシステム。

【請求項 8】ヘッダ部に、請求項 1 または 6 に記載の電子メール鍵登録装置のアドレスを含むことを特徴とする電子メール。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、インターネット等の広域オープンネットワークにおいて、電子メールに係る鍵を登録する装置、電子メールを送受する装置、および電子メールシステムに関するものである。

【0002】

【従来の技術】インターネットにおける従来の電子メールシステムにおいては、電子メールは基本的に送りっぱなしであり、受信人が返信を行なわない限り、送信人は自分が送信した電子メールが受信人に正しく届けられたか、また受信人がその内容を読んだか、確認することはできない。また、一度送信した電子メールは送信人が制御することは基本的に不可能であり、例えば受信人が読む前にその電子メールを取り消す、あるいは内容を修正することはできない。

【0003】

【発明が解決しようとする課題】商用 BBS (Bulletin Board System) 等の閉じたネットワークにおける電子メールシステムにおいては、ネットワーク全体の管理者が存在する。したがって、送信したメールもこの管理者の管理下にあるから、受信人に正しく届けられたか、また受信人が内容を読んだか確認することが可能であり、さらに受信人が読む前であれば取り消すことも可能である。

【0004】ところが、インターネット等のネットワークの集合体においては、集合体全体の管理者が存在しないため、送信したメールが、送信人が属するネットワークを離れると、取り消し等の制御は不可能であり、また受信人が読んだか確認することはできない。

【0005】本発明の目的は、インターネット等における電子メールシステムにおいても、閉じたネットワーク同様の機能、すなわち送信人が送信した電子メールが正しく受信人に届けられたか確認する機能、受信人がその内容を読んだか確認する機能、および電子メールの取り消し等の制御機能を提供することである。

【0006】

【課題を解決するための手段】上記目的を達成するため、請求項1に係る電子メール鍵登録装置は、電子メールの送信人からの要求にしたがって、各々の電子メール固有のメッセージIDをキーとして鍵を登録し、または削除する手段と、鍵が削除されていない場合に限り、電子メールの受信人からの要求にしたがって、登録されている鍵を前記受信人に送る手段と、登録された鍵それぞれについて、前記受信人が鍵を要求したか否かを前記送信人に通知する手段とを備えたことを特徴とする。

【0007】請求項2に係る電子メール送信装置は、電子メールの送信人が電子メールの送信操作を行なうたびに鍵を生成し、この鍵を用いて電子メールを暗号化し受信人に送信する手段と、前記電子メールのメッセージIDと前記鍵を請求項1に記載の鍵登録装置に鍵登録要求として送信する手段と、前記鍵登録装置からの通知に基づいて、送信済みの電子メールそれぞれについて、受信人が鍵を要求したか否かを表示する手段と、受信人が鍵を未だ要求していない電子メールについては、送信人が取消操作を行なうと、この鍵の削除要求を鍵登録装置へ送り、受信人が読むことを不可能にする手段とを備えたことを特徴とする。

【0008】請求項3に係る発明は、請求項2に記載の送信装置によって暗号化され送信された電子メールを受信する電子メール受信装置であって、受信人が閲覧操作を行なったとき、受信した電子メールに対応する鍵を前記鍵登録装置に対して自動的に要求し、該鍵を取得する手段と、取得した鍵を用いて電子メールを復号化する手段とを備えたことを特徴とする。

【0009】請求項4に係る発明は、請求項2に記載の電子メール送信装置において、前記暗号化した電子メールのハッシュ値を算出し、このハッシュ値を、メッセージIDおよび鍵と共に鍵登録要求として前記鍵登録装置に送信することを特徴とする。

【0010】請求項5に係る発明は、請求項3に記載の電子メール受信装置において、受信人が閲覧操作を行なったとき、受信した電子メールのハッシュ値を受信人固有の秘密鍵を使って暗号化したものを、前記電子メールのメッセージIDと共に鍵要求として、前記電子メールに対応する鍵登録装置に送信することを特徴とする。

【0011】請求項6に係る発明は、請求項1に記載の電子メール鍵登録装置において、請求項4に記載の電子メール送信装置が送信したメッセージID、鍵、およびハッシュ値を受信し、前記メッセージIDをキーとして前記鍵およびハッシュ値を記録し、請求項5に記載の電子メール受信装置が送信したメッセージID、および暗号化されたハッシュ値を受信し、前記暗号化されたハッシュ値を受信人の公開鍵を用いて復号化したものが、前記メッセージIDをキーとして検索を行なって取り出したハッシュ値と一致するときに限り、検索を行なって取り出した鍵を前記電子メール受信装置に送信し、前記電

子メール送信装置が送信したハッシュ値と、前記電子メール受信装置が送信した暗号化されたハッシュ値を復号化したものが一致したか否かを前記電子メール送信装置に伝えることを特徴とする。

【0012】請求項7に係る電子メールシステムは、請求項1、2、3または請求項4、5、6に記載の、電子メール鍵登録装置、電子メール送信装置、および電子メール受信装置を含むことを特徴とする。

【0013】請求項8に係る電子メールは、ヘッダ部に、請求項1または6に記載の電子メール鍵登録装置のアドレスを含むことを特徴とする。

【0014】

【発明の実施の形態】以下、図面を用いて、本発明の実施の形態を説明する。まず、本実施の形態の概要を説明する。

【0015】本実施の形態では、電子メールを暗号化した上で送信する。受信側では、鍵がなければこの電子メールを読むことはできない。したがって、鍵を送信側が管理することによって、送信した電子メールを間接的に制御することが可能となる。

【0016】送信人は、送信する電子メール毎に自動生成した鍵を用いて電子メールを暗号化した上で、受信人に送信する。そしてこの鍵を、送信人が属するネットワーク内に設置した鍵登録装置に登録する。この鍵登録装置は、インターネットを介して、送信人が属するサイトの外からアクセスすることができる。正当な受信人からのアクセスであると確認された場合は、送信人が登録した鍵を受信人に送信する。正当な受信人からのアクセスがあったということは、当該電子メールが正しく受信人に届けられ、かつ受信人が電子メールを見る意思があることを意味するから、鍵登録装置は、送信人に対し開封通知を送る。送信人は、開封通知を受け取ることにより、自分が送った電子メールが正しく受信人に届けられ、かつ受信人が電子メールを見る意思があることを知ることができる。

【0017】受信人の認証方法としては様々な方法が考えられるが、個々の電子メール固有のメッセージIDを用いる方法が簡便な方法である。つまり、メッセージIDを知っている者は正しい受信人であるとみなす。ただし、この方法では、電子メールを盗み読みした第三者が、その電子メールのメッセージIDを鍵登録装置に送って鍵を取得し、電子メールを復号化することが可能である。第三者による盗み読みが問題となる場合は、公開鍵暗号系を利用して受信人の認証を行なうようにする。つまり受信人は、メッセージIDと共に、受信した電子メールのハッシュ値を公開鍵暗号系における受信人の秘密鍵で暗号化したものを、鍵登録装置に送る。鍵登録装置は、この暗号化したハッシュ値を、受信人の公開鍵で復号化したものが、事前に送信人が登録したハッシュ値に一致することを確認する。これらのハッシュ値が一致

するのであれば、正当な受信人であることが保証されるから、その場合のみ、鍵を受信人に送るようにする。

【0018】ハッシュ値の計算方法としては、RAS Data Security社のRon Rivest氏が発明したMD5（メッセージダイジェスト関数5）等を用いることができる。公開鍵暗号系としては、RSA等を用いることができる。

【0019】このような、受信人が電子メールのハッシュ値を鍵登録装置に送る方法の場合、このハッシュ値を送信人に送れば、内容証明郵便と同等の機能を持たせることができる。つまり、受信人が正しいハッシュ値を算出できたということは、送信人が送った電子メールの内容が正しく受信人に届けられたということであり、このことを、第三者に対して証明することができる。

【0020】盗み読みが問題となる場合、通信路をバーチャルプライベートネットワーク技術を用いて暗号化し、この通信路経由で電子メールを送っても良い。この場合、受信人以外の第三者が電子メールのメッセージIDを知ることは事実上不可能であるから、正しいメッセージIDを知っている者は正しい受信人であるとみなすことができる。なお、バーチャルプライベートネットワーク技術とは、インターネット上に仮想的な通信路を設け、そこを通るデータはすべて暗号化することにより、データの盗み読みができないようにする技術である。

【0021】図面を用いて、本実施の形態について、詳しく説明する。図1は、インターネットにおいて内容証明つき電子メールを送る実施の形態の構成図を示す。

【0022】サイトA（図中100）のユーザ（送信人）が、ネットワーク150（この実施の形態においてはインターネット）を介して接続されているサイトB160のユーザ（受信人）宛に、内容証明つき電子メールを送る例について説明する。内容証明つきとは、電子メールが正しく届けられたと言う事実、およびその電子メールの内容を、電子メールの発信者が第三者に対して証明することが可能であることを言う。

【0023】図1において、メール送信装置110は、鍵生成装置111、暗号化装置114、ハッシュ値算出装置115を含む。鍵生成装置111は、鍵をランダムに生成する。暗号化装置114は、鍵生成装置111で生成した鍵を用いて、メール113を暗号化する。メール送信装置110は、メール113を暗号化したものをサイトB160へ送信すると共に、暗号化するとき用いた鍵を鍵登録装置120へ登録する。ハッシュ値算出装置115は、暗号化されたメールからハッシュ値を算出し、鍵登録装置120へ登録する。各メールには、メールのヘッダ部に、ユニークなメッセージIDおよび鍵登録装置120のアドレス（URL: Universal Resource Locator）を記載する。ヘッダ部は暗号化の対象から除外する。

【0024】図5に、メール113の例を示す。メール

はヘッダとそれに続く本文からなり、空行がヘッダの終りを表す。ヘッダの各フィールドの意味を次に説明する。「From:」、「To:」は、それぞれ送信人、受信人のアドレスを示す。「Date:」はメールを出した日時、「Subject:」はメールの題名を示す。「Message-ID:」は電子メールに固有のメッセージIDであり、「X-KeyServer:」は鍵登録装置120のアドレスを示す。なお、鍵登録装置120のアドレスをメール毎に記載する代わりに、DNS（Domain Name Service）等のメール受信装置からアクセス可能なデータベースに登録しても良い。メールのヘッダに鍵登録装置120のアドレスを記載しているので、使用する鍵登録装置120を使い分けることができる。例えば、メールによっては機密性の高い鍵登録装置を指定するというような使い方が可能になる。

【0025】図3に、メール送信装置110のフローチャートを示す。メール送信装置110は、ユーザの各操作（メール作成310、メール送信320、送信済みメール一覧330）に対してそれぞれ対応する処理を行なう。ユーザがメール作成操作を行なうと、ステップ310からステップ311に進み、メールの作成を行なうことができる。

【0026】ユーザが送信操作を行なうと、ステップ320からステップ321に進む。ステップ321において、鍵生成装置111は、メールごとに異なる128ビット長の鍵112をランダムに発生する。また、メール送信装置110は、電子メールに固有のメッセージIDを生成する。次に、ステップ322で、この鍵112を用いて、暗号化装置114によりメール113を暗号化する。

【0027】鍵は、必ずしもランダムである必要はなく、受信人およびこのメールを盗み読みしようとする者にとって、推測することが事実上不可能な値であればよい。暗号化アルゴリズムとしては、国際データ暗号化アルゴリズム（IDEA: International Data Encryption Algorithm）を用いる。IDEAの代わりに、他の秘密鍵暗号系アルゴリズムを用いてもよい。例えば、データ暗号化標準（DES: Data Encryption Standard）等が利用可能である。

【0028】ステップ322の後、ステップ323で、暗号化されたメールはハッシュ値算出装置115に送られ、ハッシュ値算出装置115は、メッセージダイジェスト関数5（MD5）を用いて、暗号化されたメールから、128ビットのハッシュ値を計算する。MD5の代わりに、他の一方向ハッシュ関数を用いてもよい。例えば、SHA（Secret Hash Algorithm）等が利用可能である。

【0029】次に、ステップ324で、暗号化されたメールは、ネットワーク150を経由してサイトB160へ送信される。また、ステップ325において、ハッシュ値は、鍵112およびメッセージIDと共に鍵登録装

置120に送られる。

【0030】再び図1を参照して、鍵登録装置120は、メール送信装置110から送られる、メッセージID(図1のi)、鍵、およびハッシュ値の組122(以下、これをレコードiと呼ぶ)を格納する記憶装置121と、メールの受信人の署名を確認するための復号化装置124を含む。

【0031】鍵登録装置120は、受信人からアクセスすることが可能であれば、どこに設置しても良く、メール送信装置110と一体化していても良い。ただし、鍵登録装置120は、受信人およびこのメールを盗み読みしようとする者から、鍵取得要求アクセス以外のアクセスが可能であってはならない。例えば、記録装置121の内容に直接アクセスすることが可能だと、受信人が正規の鍵取得要求を行なうことなく、鍵を取得することが可能となってしまう。したがって、鍵登録装置120は、ファイアウォールに守られたサイト内に設置すると良い。

【0032】図2に、鍵登録装置のフローチャートを示す。まずステップ201の初期化において、記憶装置121の内容をクリアする。ステップ202で、メール送信装置110あるいは受信装置160からのアクセスを待つ。

【0033】メール送信装置110から鍵登録要求があった場合、ステップ204において、メール送信装置110から送られてきたメッセージID i、鍵、およびハッシュ値hを受けとり、これをレコードiとして記憶装置121に登録する。各レコードはメッセージID iで検索可能としておく。つまり任意のiに対し、対応するレコードiを取り出すことができるようにしておく。

【0034】メール送信装置110から鍵取消要求があった場合は、ステップ206において、メール送信装置110からメッセージID iを受けとり、当該メッセージID iに対応するレコードiを削除する。メール受信装置160から鍵取得要求があった場合については後述する。アクセスがなければ、ステップ202に戻り、再びアクセス待ちとなる。

【0035】図3のステップ324でメール送信装置110からサイトB160のユーザ宛に送られたメールは、メール受信装置170に到達する。図1を参照して、メール受信装置170は、ハッシュ算出装置171、署名装置173、および復号化装置174を含む。

【0036】図4に、メール受信装置170のフローチャートを示す。メール受信装置170では、ステップ400で初期化を行なった後、ステップ410でユーザのメール一覧操作を検出したときには、ステップ411で、受信したメールの一覧表示を行なう。メール受信装置170は、一覧操作以外の操作(ステップ430)が可能であっても良い。例えば、メール送信装置を含んでも良く、その場合、ステップ430においてメール

送信装置の処理を行なう。

【0037】ステップ411において表示した受信メールの一覧の中から、ユーザは読みたいメールを選択し、閲覧操作を行なうことができる。ユーザによる閲覧操作が行なわれたときには、ステップ420からステップ421に進む。ステップ421で、閲覧が指示されたメールが開封済みか否か判定する。そのメールが既に開封済み(復号化済み)のメールであれば、ステップ427に進み、そのまま表示する。そうでない場合は、まず復号化してから表示する。復号化のための処理を次に説明する。

【0038】ステップ422において、ハッシュ値算出装置171は、ハッシュ値算出装置115と同じハッシュ関数を用いて、届いたメールのハッシュ値を求める。ステップ423で、署名装置173により、このハッシュ値を、受信人の秘密鍵172を用いて暗号化する。

【0039】暗号化アルゴリズムとしてはRSAを用いる。RSAの代わりに、他の公開鍵暗号系アルゴリズムを用いてもよい。例えば、楕円関数に基づく暗号等が利用可能である。受信人の秘密鍵172に対応する公開鍵123は、あらかじめ公の認証証明機関に登録し、誰でも参照できるようにしておく。公開鍵の登録場所の例として、日本ペリサイン・デジタルIDセンターや、PGPの公開鍵サーバなどがあげられる。受信人の秘密鍵172を用いて署名装置173が暗号化したハッシュ値は、受信人の署名と同等の効力を持つ。これをデジタル署名と呼ぶ。つまり、署名が受信人の公開鍵で復号化できるのであれば、その署名を作った人は、その受信人であることが保証できる。

【0040】ステップ424において、前述した署名を、受信したメールのヘッダ部に記載されているメッセージID iと共に、同じくヘッダ部に記載されているアドレスの鍵登録装置120に対して、鍵取得要求として送信する。

【0041】図2を参照して、鍵登録装置120において、メール受信装置170から鍵取得要求があった場合、メール受信装置からメッセージID iおよび署名sを受けとり、ステップ207からステップ208に進む。ステップ208では、レコードiを記憶装置121から検索する。ステップ209において、レコードiが記憶装置121に存在しない場合、送信者によって電子メールの取消が行なわれたとみなし、ステップ202に戻る。

【0042】レコードiが記憶装置121に存在した場合は、ステップ210において、復号化装置124により署名sを受信人の公開鍵を用いて復号化する。受信人の公開鍵は、必要に応じて公の認証証明機関から取得する。あるいは送信人があらかじめ適当な手段によって

(例えば、直接受信人に会ったときに手渡しで取得する等)受信人の公開鍵を取得し、メールを送信する際に鍵

登録装置 1 2 0 に登録しても良い。

【0 0 4 3】復号化した署名 C (s) が、レコード i に登録してあるハッシュ値 h と一致するならば、正しい受信人からの鍵要求と判断できる。ステップ 2 1 0 で C

(s) = h であったときは、ステップ 2 1 1 において、レコード i に登録されている鍵 1 1 2 をメール受信装置 1 7 0 に返送し、署名 s を開封通知 1 1 6 としてメール送信装置 1 1 0 に送る。なお、鍵 1 1 2 をメール受信装置 1 7 0 に返送する際には、受信人の公開鍵により暗号化して送る。ステップ 2 1 0 で署名 C (s) がハッシュ値 h と一致しない場合、不正な鍵要求と判断し、ステップ 2 0 2 に戻る。

【0 0 4 4】図 4 に戻って、メール受信装置 1 7 0 のステップ 4 2 5 において、鍵登録装置 1 2 0 から鍵 1 1 2 (受信人の公開鍵により暗号化されている) が返送されてきた場合は、ステップ 4 2 6 でこの鍵を複合化し、複合化した鍵を用いて復号化装置 1 7 4 により前述した受信メールを復号化する。ステップ 4 2 7 では、複合化した受信メールを受信人に対して表示する。鍵が返送されてこなかった場合は、鍵が送信人によって取り消されたものとみなし、ステップ 4 2 5 からステップ 4 2 8 に進み、ユーザに対して取消通知を表示する。

【0 0 4 5】図 3 に戻って、メール送信装置 1 1 0 は、ステップ 3 2 0 ~ 3 2 5 により送信したメールそれぞれを送信済みメールとして記録する。送信人が一覧操作を行なったときは、ステップ 3 3 0 からステップ 3 3 1 に進み、送信済みメールの一覧を表示する。それぞれのメールには、開封通知 1 1 6 を鍵登録装置から受けとったか否かを示すフラグを表示する。

【0 0 4 6】開封通知を受けとっていないメールに対しては、送信人はそのメールを取り消すことができる。ステップ 3 3 1 で表示されたメール一覧の画面で、取消操作を行なうと、ステップ 3 3 2 からステップ 3 3 3 に進み、メール送信装置 1 1 0 は鍵登録装置 1 2 0 に対して鍵取消要求を送信する。この鍵取消要求に対し、鍵登録装置 1 2 0 は、ステップ 2 0 5 からステップ 2 0 6 に進み、取消を指定されたレコード i を削除する。

【0 0 4 7】ステップ 3 4 0 において、鍵登録装置 1 2 0 から開封通知 1 1 6 が送られてきた場合は、ステップ 3 4 1 でそれを記録し、ステップ 3 3 1 で表示する送信済みメール一覧に反映させる。

【0 0 4 8】本実施の形態を、ISO 9 0 0 0, ISO 1 4 0 0 0 等の規格の適合認証へ応用した実施例を次に説明する。図 6 に、その構成図を示す。

【0 0 4 9】上述の規格の適合認証においては、審査を受ける側の受査サイトは、まず管理マニュアルを審査機関に送付する。審査機関は、この管理マニュアルが規格に適合しているか審査し、所見報告をメールで受査サイトへ送るわけであるが、所見報告には一定期間内に受査

サイトが対応すべき事項が書かれている。ネットワーク上のトラブル等で所見報告が受査サイトに届かない、あるいは届くのが遅れると審査計画が狂う。

【0 0 5 0】そこで、上述の実施の形態を適用して、図 6 に示すように、審査機関 6 1 0 がメール送信装置 6 1 1 を使って送るメールを暗号化し、その鍵を鍵登録装置 6 1 2 に登録する。メールを受信した受査サイト 6 3 0 は、鍵要求を前記鍵登録装置 6 1 2 に送り鍵を取得してメールを復号化する。

【0 0 5 1】審査機関 6 1 0 は、鍵登録装置 6 1 2 に届く鍵要求を監視することにより、受査サイト 6 3 0 がいつメールを読んだか把握することができる。一定時間以上たっても鍵要求が届かない場合は、メール配送上のトラブル、あるいは受査サイト 6 3 0 が読むのを忘れている等の原因で、受査サイト 6 3 0 がメールを読んでいないと判断できる。その場合は、電話等のメール以外の手段で問い合わせを行えば良い。

【0 0 5 2】

【発明の効果】以上説明したように、本発明によれば、受信人の署名が、送信人の属するサイトへ送付されることから、送信人はメールが正しく受信人に届けられたということと、送った電子メールの内容を、第三者に対して証明することができる。また、受信人がメールを読む前であれば、送信人は鍵登録装置に登録した鍵を削除することにより、受信人がそのメールを読むことを不可能にすることができる。本発明を ISO 9 0 0 0, ISO 1 4 0 0 0 等の規格の適合認証へ応用すれば、審査機関は各受査サイトへ出したメールが正しく読まれているか常に把握することが可能になり、計画通りの審査が可能になる。

【図面の簡単な説明】

【図 1】本発明の実施の形態である電子メールシステムのブロック図。

【図 2】鍵登録装置のフローチャート図。

【図 3】電子メール送信装置のフローチャート図。

【図 4】電子メール受信装置のフローチャート図。

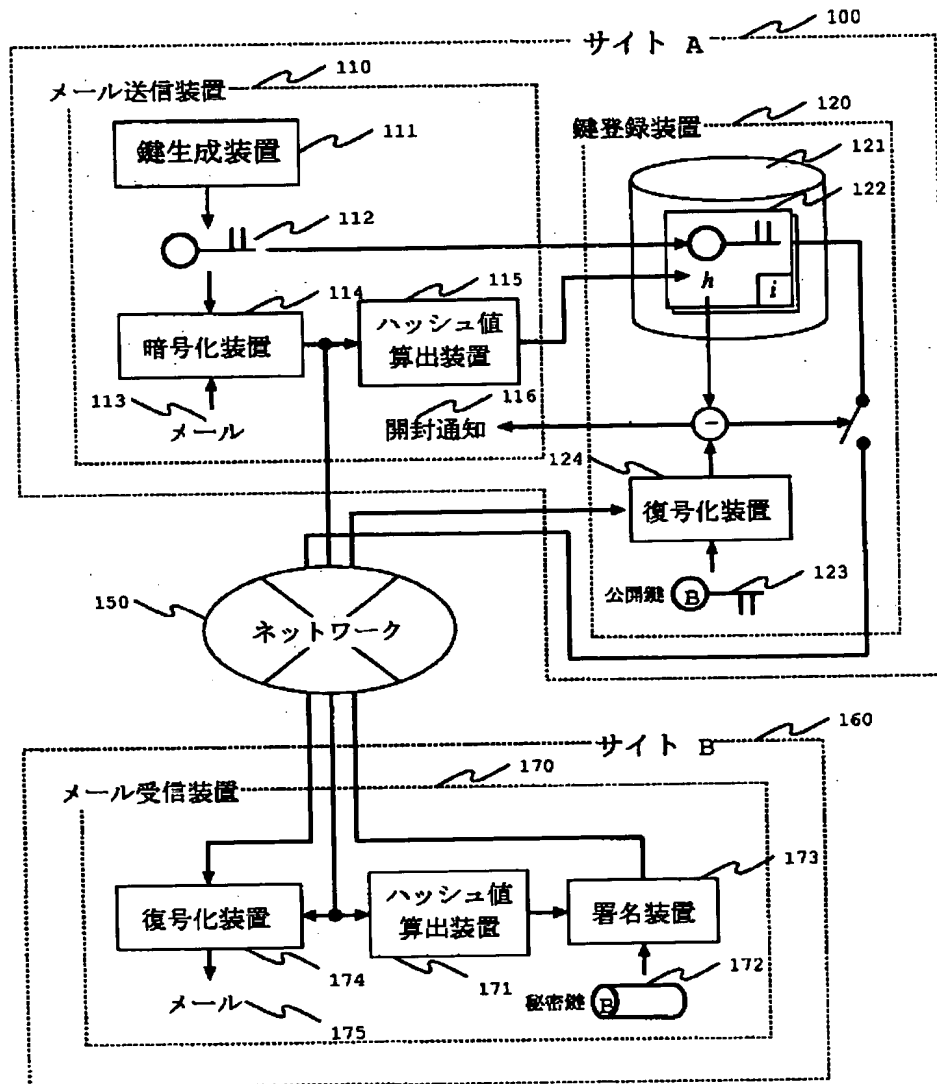
【図 5】電子メールの例を示す図。

【図 6】規格の適合認証へ応用した例を示す図。

【符号の説明】

1 0 0 … サイト A、1 1 0 … メール送信装置、1 1 1 … 鍵生成装置、1 1 2 … 鍵、1 1 3 … メール、1 1 4 … 暗号化装置、1 1 5 … ハッシュ値算出装置、1 1 6 … 開封通知、1 2 0 … 鍵登録装置、1 2 1 … 記憶装置、1 2 2 … レコード、1 2 3 … 公開鍵、1 2 4 … 複合化装置、1 5 0 … ネットワーク、1 6 0 … サイト B、1 7 0 … メール受信装置、1 7 1 … ハッシュ値算出装置、1 7 2 … 秘密鍵、1 7 3 … 署名装置、1 7 4 … 複合化装置、1 7 5 … メール。

【図 1】

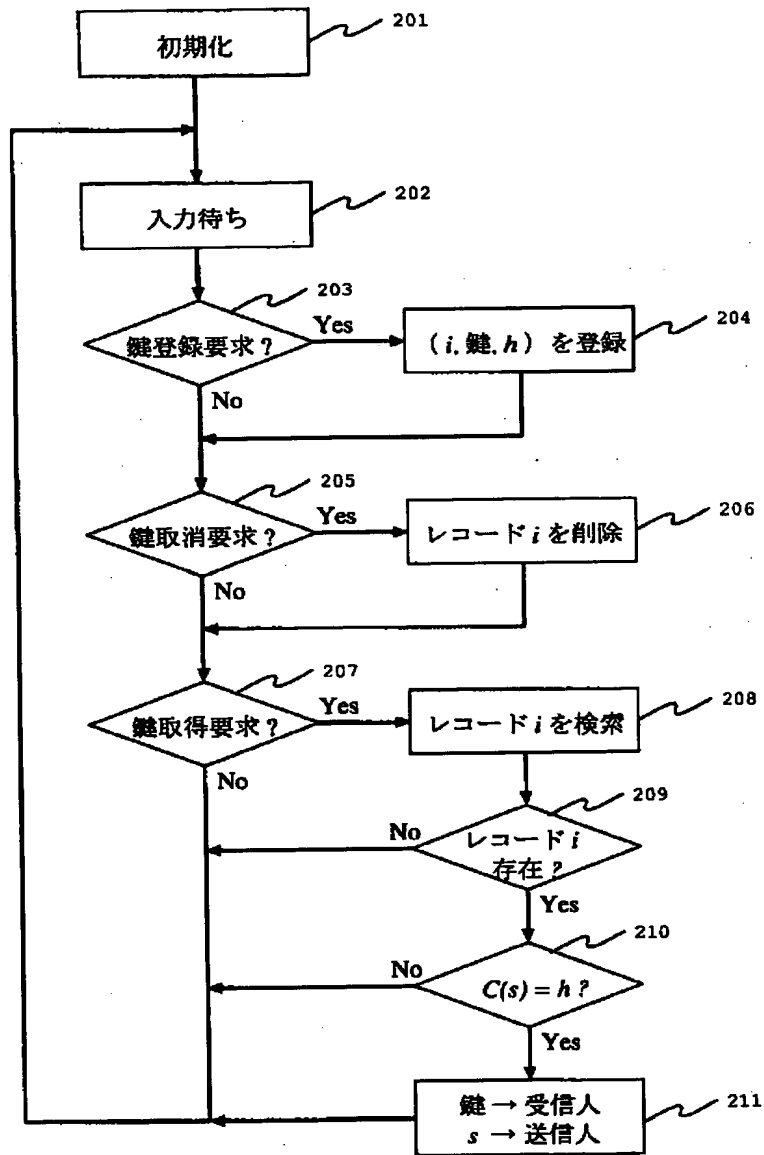


【図 5】

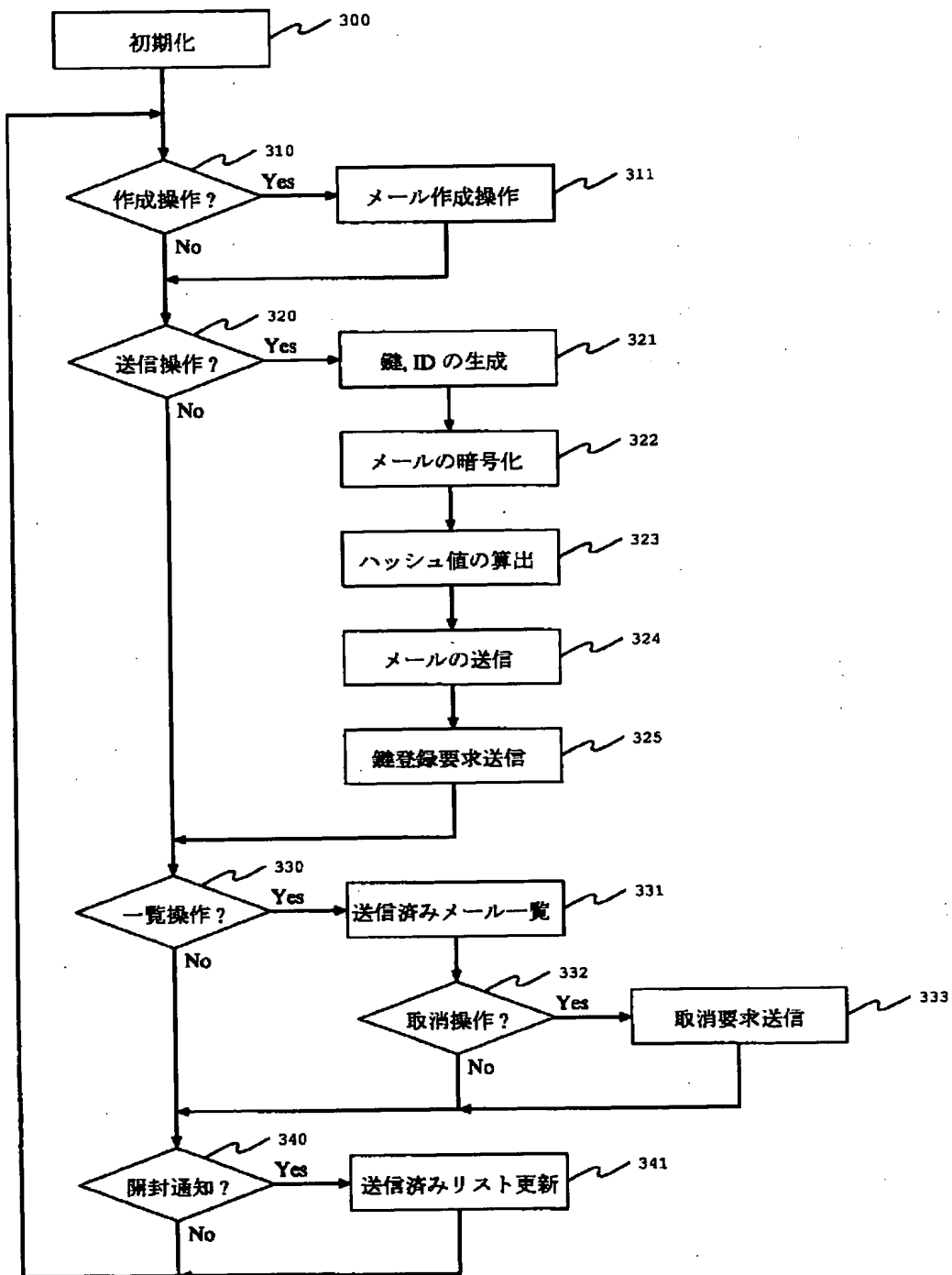
From: foo@site-A.co.jp
 To: bar@site-B.co.jp
 Date: Mon, 12 May 1997 12:01:21 +0900
 Subject: A Sample of Contents-certified Mail
 Message-ID: <199705120301.MAA20042@site-A.co.jp>
 X-KeyServer: http://www.site-A.co.jp/keys/

これは内容証明郵便のテストです。

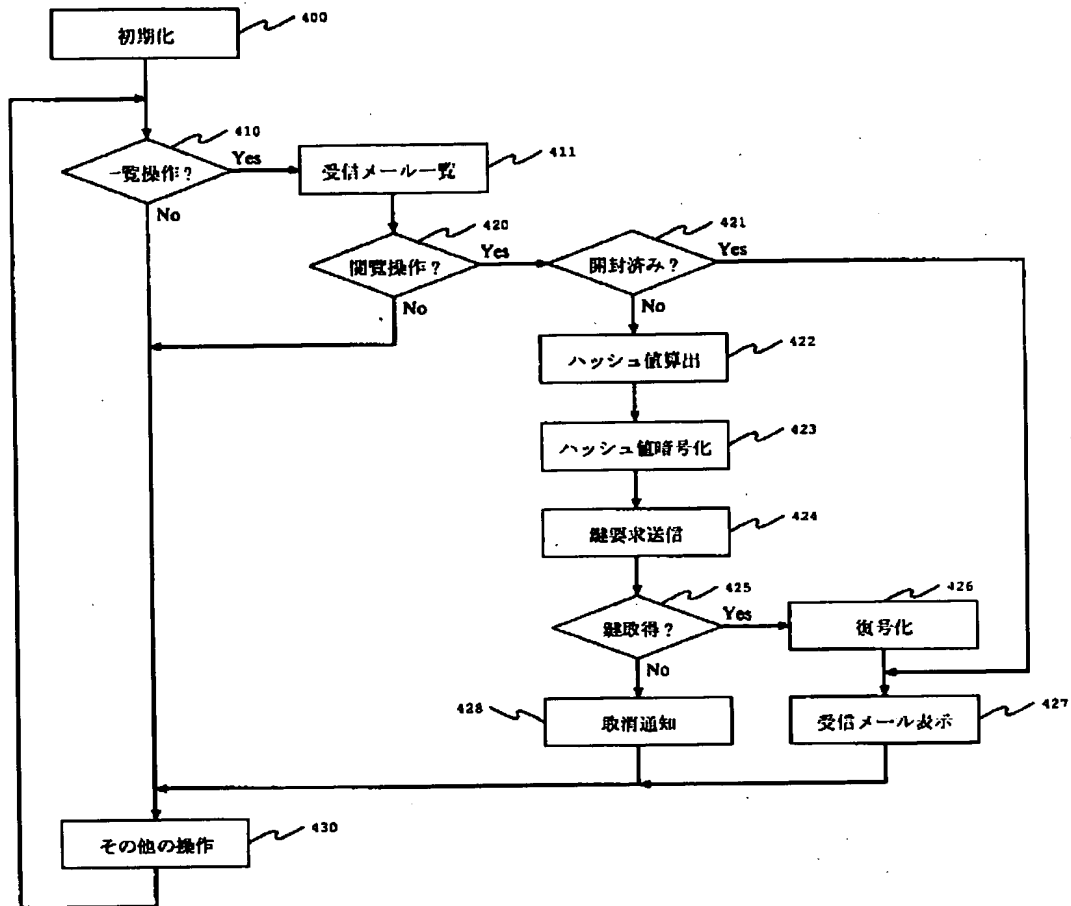
【図2】



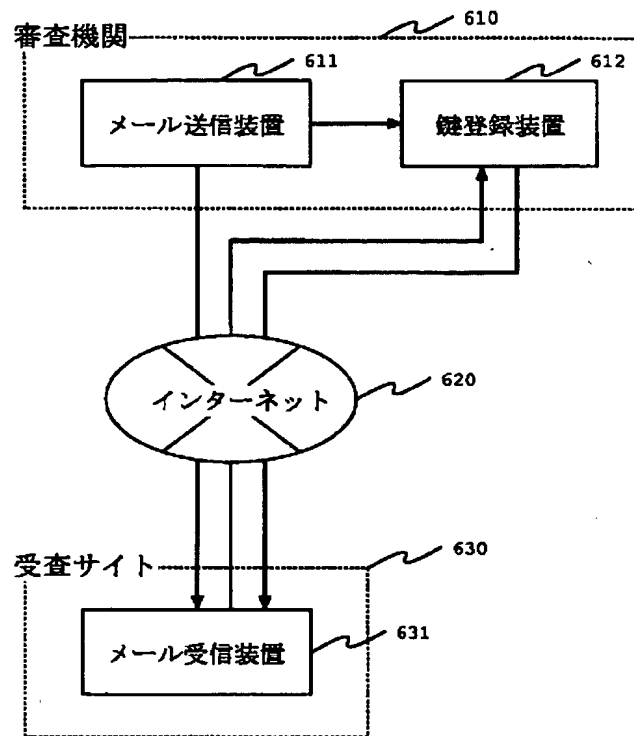
【図 3】



【図 4】



【図 6】



フロントページの続き

(51)Int.Cl.⁶

識別記号

F I
H 0 4 L 9/00

6 7 5 D